CLAIMS:

1. A method of providing a key container by a key container directory, the key container to be used to secure a message that will be sent from a sender to a recipient, the method comprising the steps of:

receiving a request for the key container from a requestor; and

in response to the request, providing a key container to the requestor that contains a cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

2. A method of providing a key container according to claim 1, wherein the key container directory is remote from the gateway, such as external to the network domain of the gateway.

3. A method of providing a key container according to claim 1 or 2, wherein the key container directory is external to the network domain of the recipient.

4. A method of providing a key container according to claim 1, 2 or 3, wherein the message is transmitted from the sender over an insecure computer network, such as the Internet.

5. A method of providing a key container according to any one of the preceding claims, wherein the network domain of the recipient is secure.

6. A method of providing a key container according to any one of the preceding claims, wherein the step of providing a key container comprises providing a key container for each gateway that the message will transit.

7. A method of providing a key container according to any one of the preceding claims, wherein the method further comprises the step of determining the identity of one or more gateways that the message will transit.

8. A method of providing a key container according to any one of the preceding claims, wherein the key container directory provides multiple key containers in the response to the request.

9. A method of providing a key container according to any one of the preceding claims, wherein the requestor is the sender of the message and the request includes the address of the recipient.

10. A method of providing a key container according to any one of the preceding claims, wherein the step of requesting the key container includes an indication that an encryption key container is requested.

11. A method of providing a key container according to any one of the preceding claims, wherein the method further comprises the step of determining what type of key container should be provided to the requestor.

12. A method of providing a key container according to claims 11, wherein the step of determining comprises determining whether the requestor is the sender of the message, and if so, providing an encryption key container to the requestor.

13. A method of providing a key container according to claims 11 or 12, wherein the step of determining further comprises determining whether the requestor is from the same domain as the gateway, and if not, providing the encryption key container containing the cryptographic key of the recipient's gateway.

14. A method of providing a key container according to claims 11, 12 or 13, wherein the step of determining further comprises determining whether the requestor is from the same domain as the gateway, and if so, providing the encryption key container having the cryptographic key of the requestor's gateway.

15. A method of providing a key container according to any one of claims 1 to 8, wherein the requestor is the gateway and the request includes the address of the sender.

16. A method of providing a key container according to any one of claims 1 to 8 or 15, wherein the step of requesting the key container includes an indication that a signing key container is requested.

17. A method of providing a key container according to any one of claims 1 to 8, 15 or 16, wherein the method further comprises the step of determining what type of key container should be provided to the requestor.

18. A method of providing a key container according to claims 17, wherein the step of determining further comprises determining whether the requestor is the gateway, and if so, providing the signing key container containing the cryptographic key of the gateway and the message sender's address.

19. A method of providing a key container according to any one of claims 1 to 8 to 15 to 18, wherein the sender's address is from the same domain as the gateway.

20. A method of providing a key container according to any one of claims 11 to 14 or 17 to 19 wherein the step of determining is based on parameters associated with the request.

21. A method of providing a key container according to any one of the preceding claims, wherein the method further comprises the step of the requestor authenticating with the key container directory.

22. A method of providing a key container according to claim 21 and limited by claim 20, wherein the step of determining is based on the information provided by the requestor when authenticating with the key container directory.

23. A method of providing a key container according to claim 21 or 22, wherein the step of authenticating is through the use of a valid username and password combination.

24. A method of providing a key container according to any one of the preceding claims, wherein once the request has been received, the method further comprises the step of generating the requested key container.

25. A method of providing a key container according to any one of the preceding claims, wherein the request is made using a computer communication protocol, such as Lightweight Directory Access Protocol (LDAP), Directory Access Protocol (DAP), Certification Management Protocol (CMP), that of XML Key Management Specification (XKMS) or the HyperText Transfer Protocol (HTTP).

26. A method of providing a key container according to any one of the preceding claims, wherein the key container contains a cryptographic key that is a public key.

27. A method of providing a key container according to any one of the preceding claims, wherein the key container is a digital certificate, such as a X.509 digital certificate.

28. A method of providing a key container according to any one of the preceding claims, wherein the key container is a Pretty Good Privacy (PGP) public key.

29. A method of providing a key container according to any one of the preceding claims, wherein the address contained in the key container is an e-mail address and the gateway is an e-mail gateway.

30. A method of providing a key container according to any one of the preceding claims, wherein the key container is provided for a specific message.

31. A method of providing a key container according to any one of the preceding claims, wherein the key container contains information that invalidates its use at a time in the future.

32. A method of providing a key container according to claim 31, wherein the time is of sufficiently short duration that the key container can be used for only a few messages.

33. A method of providing a key container according to any one of the preceding claims, wherein the key container contains the same container identifiers, such as serial number and issuer name, of the key container of the gateway.

34. A method of providing a key container according to any one of claims 1 to 14 or 20 to 33, wherein the key container is an encryption key container to be used for encryption operations.

35. A method of providing a key container according to claim 34, wherein the key container contains a parameter that indicates that the key container is to be used for encryption functions.

36. A method of providing a key container according to any one of claims 1 to 14 or 20 to 35, wherein the key container secures the message through use of the cryptographic key to encrypt the message.

37. A method of providing a key container according to any one of claims 1 to 14 or 20 to 36, wherein the sender's address is from the same domain as the gateway.

38. A method of providing a key container according to any one of claims 1 to 8 or 15 to 33, wherein the key container is a signing key container.

39. A method of providing a key container according to any one of claims 1 to 8, 15 to 33 or 38, wherein the key container contains a parameter that indicates that the key container is to be used for signing operations.

40. A method of providing a key container according to any one of claims 1 to 8, 15 to 33, 38 or 39, wherein the key container secures the message by permitting the recipient to perform signature verification upon the message.

41. A method of providing a key container according to any one of claims 1 to 8, 15 to 33, 38, 39 or 40, wherein the key container includes information that permits a requestor to determine the authenticity and integrity of the key container.

42. A method of providing a key container according to any one of the preceding claims, wherein the key container contains security preferences of the gateway, such as Secure Multipart Internet Mail Extensions (S/MIME) Capabilities or PGP Symmetric Algorithm Preferences.

43. A method of providing a key container according to any one of the preceding claims, wherein the key container includes information about the key container directory that provided the key container.

44. A key container directory operable to provide a key container according to the method described in any one of the preceding claims, wherein the key container directory is remote from the gateway, such external to the network domain of the gateway.

45. A key container directory according to claim 44, wherein the key container has a datastore of cryptographic keys that can be contained in any provided key container.

46. A method of receiving a key container comprising the steps of:

sending a request to a key container directory for a key container to be used to secure a message that is transmitted from a sender to a recipient; and

receiving from the key container directory the key container that contains the cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

47. A method of receiving a key container according to claim 46, wherein the method is performed by the sender of the message.

48. A method of receiving a key container according to claim 46 or 47, wherein the step of sending a request for the key container includes an indication that an encryption key container is requested.

49. A method of receiving a key container according to claim 46, 47 or 48, wherein the step of sending the request for the key container includes the address of the recipient.

50. A method of receiving a key container according to any one of claims 46 to 49, wherein the method further comprises the step of encrypting the message using the cryptographic key contained in the key container.

51. A method of receiving a key container according to any one of claims 46 to 50, wherein the key container is an encryption key container to be used for encryption operations.

52. A method of receiving a key container according to any one of claims 46 to 51, wherein the key container contains a parameter that indicates that the key container is to be used for encryption functions.

53. A method of receiving a key container according to any one of claims 46 to 52, wherein the key container secures the message through use of the cryptographic key to encrypt the message.

54. A method of receiving a key container according to any one of claims 46 to 53, wherein the sender's address is from the same domain as the gateway.

55. A method of receiving a key container according to claim 46, wherein the method is performed by the gateway.

56. A method of receiving a key container according to claim 46 or 55, wherein the step of sending the request for the key container includes an indication that a signing key container is requested.

57. A method of receiving a key container according to claim 46, 55 or 56, wherein the step of sending the request for the key container includes the address of the sender.

58. A method of receiving a key container according to any one of claims 46 or 55 to 57, wherein the key container is a signing key container.

59. A method of receiving a key container according to any one of claims 46 or 55 to 58, wherein the key container contains a parameter that indicates that the key container is to be used for signing operations.

60. A method of receiving a key container according to any one of claims 46 or 55 to 59, wherein the key container secures the message by permitting the recipient to perform signature verification upon the message.

61. A method of receiving a key container according to any one of claims 46 to 60, wherein the key container includes information that permits a requestor to determine the authenticity and integrity of the key container.

62. A method of receiving a key container according to any one of claims 46 to 61, wherein the key container contains security preferences of the gateway, such as Secure Multipart Internet Mail Extensions (S/MIME) Capabilities or PGP Symmetric Algorithm Preferences.

63. A method of receiving a key container according to any one of claims 46 to 62, wherein the key container includes information about the key container directory that provided the key container.

64. An e-mail client that is operable to perform the method of receiving a key container as according to any one of claims 46 to 54.

65. A gateway that is operable to perform the method of receiving a key container according to any one of the claims 46 or 55 to 60.

66. A key container to be used to secure a message that is transmitted from a sender to a recipient using a gateway, wherein the key container contains a cryptographic key of the gateway, an address of the sender or the recipient and information that invalidates the use of the key container at a time in the future.